



Cisco PIX Security Appliance Release Notes Version 8.0(2)

June 2007

Contents

This document includes the following sections:

- [Introduction, page 1](#)
- [System Requirements, page 2](#)
- [New Features, page 5](#)
- [Important Notes, page 8](#)
- [Caveats, page 10](#)
- [Related Documentation, page 13](#)
- [Obtaining Documentation and Submitting a Service Request, page 13](#)

Introduction



Note

The PIX 501, PIX 506/506E, and PIX 520 security appliances are not supported in software Version 8.0(2).

The Cisco PIX 500 series security appliance delivers unprecedented levels of defense against threats to the network with deeper web inspection and flow-specific analysis, improved secure connectivity through end-point security posture validation and voice and video over VPN support. It also provides enhanced support for intelligent information networks through improved network integration, resiliency, and scalability.

For more information on all the new features, see [New Features, page 5](#).



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007 Cisco Systems, Inc. All rights reserved.

Additionally, the adaptive security appliance software supports Cisco Adaptive Security Device Manager (ASDM). ASDM delivers world-class security management and monitoring through an intuitive, easy-to-use web-based management interface. Bundled with the security appliance, ASDM accelerates adaptive security appliance deployment with intelligent wizards, robust administration tools, and versatile monitoring services that complement the advanced integrated security and networking features offered by the market-leading suite of the security appliance. Its secure, web-based design enables anytime, anywhere access to security appliances.

System Requirements

The sections that follow list the system requirements for operating a security appliance.



Note

The PIX 501, PIX 506/506E, and PIX 520 security appliances are not supported in software Version 8.0(2).

Memory Requirements

If you are using a PIX 515/515E running PIX Version 6.2/6.3, you must increase your memory before upgrading to PIX Version 8.0(2). This version requires at least 64 MB of RAM for Restricted (R) licenses and 128 MB of RAM for Unrestricted (UR) and Failover (FO) licenses. [Table 1](#) lists the default value for the memory that ships with each security appliance and flash memory requirements for Version 8.0(2).

Table 1 Default Memory Shipped and Flash Memory Requirements

| PIX Security Appliance Model | Default Memory (MB) | Flash Memory Required (MB) |
|------------------------------|---------------------|----------------------------|
| 515/515E | 64 | 16 |
| 525 | 128 | |
| 535 | 512 | |

For more information about minimum memory requirements, see the “Minimum Memory Requirements” section in the *Guide for Cisco PIX 6.2 and 6.3 Users Upgrading in Cisco PIX Software Version 7.0*.

Software Requirements

Version 8.0(2) requires the following:

- The minimum software version required before upgrading to PIX Version 8.0(2) is PIX Version 7.2. If you are running a PIX version earlier than Version 6.2, you must first upgrade to PIX Version 6.2 or PIX Version 6.3 before you can upgrade to PIX Version 7.2.
- To upgrade your PIX software image, go to the following website:
<http://www.cisco.com/public/sw-center/index.shtml>
- For information on specific licenses supported on each model of the security appliance, go to the following website: <http://www.cisco.com/en/US/docs/security/asa/asa80/license/license80.html>

- If you are upgrading from a previous PIX version, save your configuration and record your activation key and serial number. For new installation requirements, go to the following website: <http://www.cisco.com/public/sw-center/index.shtml>

Maximum Recommended Configuration File Size

For the PIX 525 and PIX 535, the maximum supported configuration file size is 2 MB for Version 8.0(2). For the PIX 515/515E, the maximum supported configuration file size is 1 MB for Version 8.0(2). If you are using ASDM, we recommend no more than a 500 KB configuration file, because larger configuration files can interfere with the performance of ASDM on your workstation.

While configuration files up to 2 MB are supported on the PIX 525 and PIX 535, be aware that such large configuration files can reduce system performance. For example, a large configuration file is likely to noticeably slow execution times in the following situations:

- While executing commands such as the **write terminal** and **show running-config** commands
- Failover (the configuration synchronization time)
- During a system reload

Cisco VPN Software Interoperability

| Cisco VPN Series | Interoperability Comments |
|------------------------------|---|
| Cisco IOS routers | Version 8.0(2) requires Cisco IOS Release 12.3(T)T or higher running on the router when using IKE Mode Configuration on the security appliance. |
| Cisco VPN 3000 concentrators | Version 8.0(2) requires Cisco VPN 3000 concentrator Version 3.6 or higher for correct VPN interoperability. |

Cisco VPN Client Interoperability

| Cisco VPN Client | Interoperability Comments |
|--|--|
| Cisco VPN client v3.x/4x (Unified VPN client framework) | Version 8.0(2) supports the Cisco VPN client Version 3.6 or higher that runs on all Microsoft Windows platforms. This version also supports the Cisco VPN client Version 3.6 or higher that runs on Linux, Solaris, and Macintosh platforms. |

Cisco Easy VPN Remote Interoperability

| Cisco Easy VPN Remote | Interoperability Comments |
|---|--|
| Cisco PIX Security Appliance Easy VPN remote V6.3 | Version 8.0(2) Cisco Easy VPN server requires the Cisco PIX security appliance Version 6.3 Easy VPN remote that runs on the PIX 501 and PIX 506 platforms. |
| VPN 3000 Easy VPN remote V3.x/4x | Version 8.0(2) Cisco Easy VPN server requires the Version 3.6 or higher of the Easy VPN remote that runs on the VPN 3002 platform. |
| Cisco IOS Easy VPN remote Release 12.2(16.4)T | Version 8.0(2) Cisco Easy VPN server interoperates with Cisco IOS 806 Easy VPN remote Release (16.4)T. |

Determining the Software Version

Use the **show version** command to verify the software version installed on your security appliance. Alternatively, you can view the software version on the Cisco ASDM home page.

Upgrading to a New Software Version

If you have a Cisco.com (CDC) login, you can obtain software from the following website:

<http://www.cisco.com/public/sw-center/index.shtml>

If you want to upgrade from Version 7.1.(x) to 7.2(x) or downgrade from Version 7.2(x) to Version 7.1(x), you must follow the subsequent procedure, because older versions of the security appliance images do not recognize new ASDM images, and new security appliance images does not recognize old ASDM images.

You can also use the CLI to download the image. For more information, see the “Downloading Software or Configuration Files to Flash Memory” section in the *Cisco Security Appliance Command Line Configuration Guide*.

To upgrade from Version 7.2.(x) to Version 8.0(2), perform the following steps:

-
- Step 1** Load the new Version 8.0(2) image from the following website:
<http://www.cisco.com/public/sw-center/index.shtml>
 - Step 2** Reload the device to upgrade to the Version 8.0(2) image.
 - Step 3** Copy the new ASDM Version 6.0 image from the following website:
<http://www.cisco.com/public/sw-center/index.shtml>
 - Step 4** Enter the following command to tell the security appliance where to find the ASDM image:
hostname(config)# **asdm image flash:/asdmfile**
-

To downgrade from Version 8.0(2) to 7.2.(x), perform the following steps:

-
- Step 1** Load the earlier Version 7.2(x) image from the following website:
<http://www.cisco.com/public/sw-center/index.shtml>

- Step 2** Reload the device to downgrade to the Version 7.2(x) image.
- Step 3** Copy the earlier ASDM Version 5.2(x) image from the following website:
<http://www.cisco.com/public/sw-center/index.shtml>
- Step 4** Enter the following command to tell the security appliance where to find the ASDM image:
- ```
hostname(config)# asdm image flash:/asdmfile
```

## New Features

This section lists the new feature for Version 8.0(2). All new features are supported in ASDM 6.0(2).

| Feature Type            | Feature                                    | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-------------------------|--------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>General Features</b> |                                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Routing                 | EIGRP routing                              | The adaptive security appliance supports EIGRP or EIGRP stub routing.                                                                                                                                                                                                                                                                                                                                                                                                       |
| High Availability       | Remote command execution in Failover pairs | You can execute commands on the peer unit in a failover pair without having to connect directly to the peer. This feature works for both Active/Standby and Active/Active failover.                                                                                                                                                                                                                                                                                         |
|                         | Failover pair Auto Update support          | You can use an Auto Update server to update the platform image and configuration in failover pairs.                                                                                                                                                                                                                                                                                                                                                                         |
|                         | Stateful Failover for SIP signaling        | SIP media and signaling connections are replicated to the standby unit.                                                                                                                                                                                                                                                                                                                                                                                                     |
|                         | Redundant interfaces                       | A logical redundant interface pairs an active and a standby physical interface. When the active interface fails, the standby interface becomes active and starts passing traffic. You can configure a redundant interface to increase the adaptive security appliance reliability. This feature is separate from device-level failover, but you can configure redundant interfaces as well as failover if desired. You can configure up to eight redundant interface pairs. |

| Feature Type (continued) | Feature (continued)                            | Description (continued)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|--------------------------|------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Access Policies          | Dynamic access policies (DAP)                  | <p>VPN gateways operate in dynamic environments. Multiple variables can affect each VPN connection, for example, intranet configurations that frequently change, the various roles each user may inhabit within an organization, and logins from remote access sites with different configurations and levels of security. The task of authorizing users is much more complicated in a VPN environment than it is in a network with a static configuration.</p> <p>Dynamic access policies (DAP) on the security appliance let you configure authorization that addresses these many variables. You create a dynamic access policy by setting a collection of access control attributes that you associate with a specific user tunnel or session. These attributes address issues of multiple group membership and endpoint security. That is, the security appliance grants access to a particular user for a particular session based on the policies you define. It generates a DAP at the time the user connects by selecting and/or aggregating attributes from one or more DAP records. It selects these DAP records based on the endpoint security information of the remote device and the AAA authorization information for the authenticated user. It then applies the DAP record to the user tunnel or session.</p> |
|                          | Administrator Differentiation                  | Lets you differentiate regular remote access users and administrative users under the same database, either RADIUS or LDAP. You can create and restrict access to the console via various methods (TELNET and SSH, for example) to administrators only. It is based on the IETF RADIUS "service-type" attribute.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Platform Enhancements    | VLAN support for remote access VPN connections | Provides support for mapping (tagging) of client traffic at the group or user level. This feature is compatible with clientless as well as IPSec and SSL tunnel-based connections.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|                          | VPN load balancing for the ASA 5510            | Extends load balancing support to ASA 5510 adaptive adaptive security appliances that have a Security Plus license.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|                          | Crypto Conditional Debug                       | Lets users debug an IPSec tunnel on the basis of predefined crypto conditions such as the peer IP address, connection-ID of a crypto engine, and security parameter index (SPI). By limiting debug messages to specific IPSec operations and reducing the amount of debug output, you can better troubleshoot the adaptive security appliance with a large number of tunnels.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| HTTP Proxy               | PAC Support                                    | Lets you specify the URL of a proxy autoconfiguration file (PAC) to download to the browser. Once downloaded, the PAC file uses a JavaScript function to identify a proxy for each URL.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| HTTPS Proxy              | Proxy Exclusion List                           | Lets you configure a list of URLs to exclude from the HTTP requests the adaptive security appliance can send to an external proxy server.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |

| Feature Type (continued) | Feature (continued)                                                             | Description (continued)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|--------------------------|---------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| NAC                      | Support for audit services                                                      | You can configure the adaptive security appliance to pass the IP address of the client to an optional audit server if the client does not respond to a posture validation request. The audit server uses the host IP address to challenge the host directly to assess its health. For example, it might challenge the host to determine whether its virus checking software is active and up-to-date. After the audit server completes its interaction with the remote host, it passes a token to the posture validation server, indicating the health of the remote host. If the token indicates the remote host is healthy, the posture validation server sends a network access policy to the adaptive security appliance for application to the traffic on the tunnel. |
| <b>Firewall Features</b> |                                                                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Application Inspection   | Modular Policy Framework inspect class map                                      | Traffic can match one of multiple match commands in an inspect class map; formerly, traffic had to match all match commands in a class map to match the class map.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|                          | TLS Proxy for SCCP and SIP                                                      | Enables inspection of encrypted traffic. Implementations include SSL-encrypted VoIP signaling (that is, Skinny and SIP) interacting with the Cisco CallManager.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|                          | SIP Enhancements for CCM                                                        | Improves interoperability with CCM 5.0 and 6.x with respect to signaling pinholes.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|                          | Full RTSP PAT Support                                                           | Provides TCP fragment reassembly support, a scalable parsing routine on RTSP, and security enhancements that protect RTSP traffic.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Access Lists             | Enhanced service object group                                                   | Lets you configure a service object group that contains a mix of TCP services, UDP services, ICMP-type services, and any protocol. It removes the need for a specific ICMP-type object group and protocol object group. The enhanced service object group also specifies both source and destination services. The access list CLI now supports this behavior.                                                                                                                                                                                                                                                                                                                                                                                                             |
|                          | Ability to rename access list                                                   | Lets you rename an access list.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|                          | Live access list hit counts                                                     | Includes the hit count for ACEs from multiple access lists. The hit count value represents how many times traffic hits a particular access rule.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Attack Prevention        | Set connection limits for management traffic to the adaptive security appliance | For a Layer 3/4 management class map, you can specify the <b>set connection</b> command.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|                          | Threat detection                                                                | You can enable basic threat detection and scanning threat detection to monitor attacks such as DoS attacks and scanning attacks. For scanning attacks, you can automatically shun attacking hosts. You can also enable scan threat statistics to monitor both valid and invalid traffic for hosts, ports, protocols, and access lists.                                                                                                                                                                                                                                                                                                                                                                                                                                     |

| Feature Type (continued) | Feature (continued)              | Description (continued)                                                                                                         |
|--------------------------|----------------------------------|---------------------------------------------------------------------------------------------------------------------------------|
| NAT                      | Transparent firewall NAT support | You can configure NAT for a transparent firewall.                                                                               |
| IPv6                     | IPv6 support for SIP             | The SIP inspection engine supports IPv6 addresses. IPv6 addresses can be used in URLs, in the Via header field, and SDP fields. |

## Important Notes

This section lists important notes related to Version 8.0(2).

### virtual http Command

The **virtual http** command has been restored. This command is needed with basic authentication when you have cascading authentication requests.

### FIPS 140-2

Version 8.0(2) has been submitted for FIPS 140-2 Level 2 validation.

### AnyConnect Client Sessions

A reestablished AnyConnect Client session fails to displace an AnyConnect Client session that is terminated abnormally (CSCsi40917).

### Open Source Software Usage

For a list of the open source software used in th ASA 8.0 release, see the *Open Source Software Licenses for ASA and PIX Security Appliances* document on Cisco.com.

### User Upgrade Guide

Before upgrading to Version 8.0(2), read the *Guide for Cisco PIX 6.2 and 6.3 Users Upgrading in Cisco PIX Software Version 7.0*. This guide includes information about deprecated features and other changes in the Cisco PIX software Version 7.0. For a list of deprecated features and user upgrade information, go to the following URL:

[http://www.cisco.com/en/US/docs/security/asa/asa70/pix\\_upgrade/upgrade/guide/pixupgrd.html](http://www.cisco.com/en/US/docs/security/asa/asa70/pix_upgrade/upgrade/guide/pixupgrd.html)



**Caution**

If you share the Stateful Failover update link with a link for regular traffic such as your inside interface, you must change your configuration before upgrading. Do not upgrade until you have corrected your configuration, because this is not a supported configuration and Version 8.0(2) treats the LAN failover and Stateful Failover update interfaces as special interfaces. If you upgrade to Version 8.0(2) with a

configuration that shares an interface for both regular traffic and the Stateful Failover updates, configuration related to the regular traffic interface will be lost after the upgrade. The lost configuration may prevent you from connecting to the adaptive security appliance over the network.

## Readme Document for the Conduits and Outbound List Conversion Tool 1.2

The security appliance Outbound and Conduit Conversion tool assists in converting configurations with the **outbound** or **conduit** command to similar configurations using ACLs. ACL-based configurations provide uniformity, optimize the ACL feature set, and provide the following benefits:

- ACE insertion capability— Provides simplified system configuration and management, which allows you to add, delete, or modify individual ACEs.
- Outbound ACLs and time-based ACLs—Provides administrators with improved flexibility for defining access control policies by adding support for outbound ACLs and time-based ACLs.
- Enabling and Disabling of ACL entries—Provides a convenient troubleshooting tool that allows administrators to test and fine-tune ACLs without the need to remove and replace ACL entries.

## Features not Supported in Version 8.0(2)

The PPTP feature is not supported in Version 8.0(2).

The TLS proxy feature is not supported on the PIX security appliance.

## Downgrade to Previous Version

To downgrade to a previous version of the operating system software (software image), use the **downgrade** command in privileged EXEC mode. Use the **downgrade** command only if you want to downgrade to a version other than 7.x.

For more information and a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.



**Caution**

Do not load a previous version of software if your PIX security appliance is currently running PIX Version 7.0 or later. If you load a software image from monitor mode onto a PIX security appliance that has a PIX Version 7.0 file system, unpredictable behavior may occur and is not supported. We strongly recommend that you use the **downgrade** command from a running PIX Version 7.0 image that facilitates the downgrade process.

## Certificates

- Symptom: SSL connections from browsers and AnyConnect fail if the certificate being used contains the following enhanced key usage “IP security IKE intermediate (1.3.6.1.5.5.8.2.2)”. This is the default way of issuing certificates via SCEP enrollment to a Microsoft 2003 Enterprise CA with the newer certificate templates.

Workaround:

- Use terminal enrollment instead of SCEP to get an ASA certificate.
- Changing the SCEP policy module on the 2003 CA may alleviate this issue.

- Symptom: If the validity date on the a certificate is issued beyond the year 2099, it will fail to authenticate and an error will be generated when attempting to authenticate it.

Workaround:

- Limit the validity period of the certificate to less than the recommended end date of 03:14:08 UTC, January 19, 2038.

- Symptom: User prompted for credentials when permstore and auto-signon are both enabled.

Conditions:

Both auto-signon and permanent-storage are enabled for the server requiring authentication.

Workaround:

- Disable auto-signon for this server. Enable auto-signon only for servers having the same login credentials as WebVPN.



#### Note

Because credentials used by auto-signon take precedence over permanent-storage of user credentials, do not enable auto signon for servers that do not require authentication or that use credentials different from the adaptive security appliance. When auto signon is enabled, the adaptive security appliance passes on the login credentials that the user entered to log into the adaptive security appliance regardless of what credentials are in user storage.

## Caveats

This section lists the open and resolved caveats for Version 8.0(2).

For your convenience in locating caveats in Cisco's Bug Toolkit, the caveat titles listed in this section are drawn directly from the Bug Toolkit database. These caveat titles are not intended to be read as complete sentences because the title field length is limited. In the caveat titles, some truncation of wording or punctuation may be necessary to provide the most complete and concise description. The only modifications made to these titles are as follows:

- Commands are in **boldface** type.
- Product names and acronyms may be standardized.
- Spelling errors and typos may be corrected.



#### Note

If you are a registered cisco.com user, view Bug Toolkit on cisco.com at the following website:

[http://www.cisco.com/cgi-bin/Support/Bugtool/launch\\_bugtool.pl](http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl)

To become a registered cisco.com user, go to the following website:

<http://tools.cisco.com/RPF/register/register.do>

## Open Caveats - Version 8.0(2)

**Table 2** Open Caveats

| DDTS Number | Software Version 8.0(2) |                                                                          |
|-------------|-------------------------|--------------------------------------------------------------------------|
|             | Corrected               | Caveat                                                                   |
| CSCsj15448  | No                      | Group-policy names with embedded space(s) are not usable                 |
| CSCsj08209  | No                      | In some instances 'clear ospf process causes traceback                   |
| CSCsj22800  | No                      | clearing shuns during an attack causes traceback                         |
| CSCsj20475  | No                      | WebVPN: Group-URL fails without a /                                      |
| CSCsi09586  | No                      | Conflict between aaa listener and http redirect commands                 |
| CSCej04099  | No                      | static xlate breaks management-access inside                             |
| CSCsg47023  | No                      | L2TP Connections with Certificates to ASA Fail to Connect                |
| CSCsg65434  | No                      | Multiple ipsec peers : PIX/ASA stops processing the IPSEC peers list     |
| CSCsh15861  | No                      | VPN client fails to connect, external DHCP server                        |
| CSCsh28991  | No                      | IKE sessions are getting stuck in AM_WAIT_DELETE state                   |
| CSCsh29836  | No                      | Clientless WebVPN traffic not transmitted out separate L2L interface     |
| CSCsh40829  | No                      | LDAP: multiple Cisco-AV-Pair need to be enforced on vpn-session          |
| CSCsh67528  | No                      | L2TP/IPSec OSX client disconnection after 45 minutes when NAT-T in used  |
| CSCsh68314  | No                      | Nac-default-access list doesn't work as expected with l2tp/ipsec         |
| CSCsi00074  | No                      | Incorrect values returned by SSL VPN OIDs                                |
| CSCsi04673  | No                      | FW may drop packets when VPN address pool overlaps with interface subnet |
| CSCsi08317  | No                      | PIX using Authentication Proxy and Wildcard causes Certificates error    |
| CSCsi12180  | No                      | SSH connections may cause interface errors (no buffer and overruns)      |
| CSCsi15611  | No                      | Traceback may occur with debugs webvpn citrix 255                        |
| CSCsi32502  | No                      | packet/byte counters are not populated for the session table of CRAS MIB |
| CSCsi43492  | No                      | ASA 7.2 CIFS: incomplete upload a file with size of ~100M for Firefox 2  |
| CSCsi51600  | No                      | Misleading prompt with radius/sdi authentication on 7.2.2                |
| CSCsi58109  | No                      | ASA requests username/password until next available aaa server found     |
| CSCsi75355  | No                      | 5505 WebVPN: hw accelerator errors with >1024 bit cert                   |
| CSCsi98464  | No                      | ASA injects another 'BrowserProtocol' keyword in ICA file                |
| CSCsi98616  | No                      | After two consecutive failovers SVC connections won't replicate          |
| CSCsi98617  | No                      | VPNFO: Standby stale sessions not removed                                |
| CSCsj01643  | No                      | IPSec VPN first auth fails when SDI SoftID is in Cleared PIN Mode        |
| CSCsj03319  | No                      | WebVPN: Infopath XML fails to open correctly                             |
| CSCsj03437  | No                      | WebVPN: RDP Icon fails after a redirect action to a Citrix Presentation  |
| CSCsj13797  | No                      | SSH connection fails when first server in AAA group is unreachable       |
| CSCsj14874  | No                      | AAA Authentication against local database working inconsistently         |

Table 2 Open Caveats (continued)

| DDTS Number | Software Version 8.0(2) |                                                                          |
|-------------|-------------------------|--------------------------------------------------------------------------|
|             | Corrected               | Caveat                                                                   |
| CSCsj19829  | No                      | WebVPN: http-proxy interferes with port-forward                          |
| CSCsj24914  | No                      | vpn-simultaneous-logins does not work when configuring PKI and no-xauth  |
| CSCeg00330  | No                      | DHCPACK in reply to DHCPINFORM might get dropped                         |
| CSCsf07135  | No                      | ASDM connection may cause packet loss                                    |
| CSCsg61719  | No                      | SNMP: Coldstart Trap is not sent                                         |
| CSCsh78681  | No                      | cosmetic memory leak on his pix                                          |
| CSCsi46292  | No                      | Coldstart trap isn't sent in failover settings                           |
| CSCsi65122  | No                      | alias with overlapping static and NAT exemption xlate errors on standby  |
| CSCsi68321  | No                      | Pix DHCP relay stops passing traffic after a period of time              |
| CSCsj01620  | No                      | Type 0 Client-ID for RA clients not supported by some DHCP servers       |
| CSCsj10869  | No                      | SNMP interface counters incorrect on PIX/ASA 7.2.2.22                    |
| CSCsg39338  | No                      | to-the-box traffic from a higher metric route Int dropped for no route.  |
| CSCsh48208  | No                      | Directly connected network missing in route table                        |
| CSCsi41045  | No                      | OSPF: default-info originate with route-map fails with next hop or sourc |
| CSCsi53577  | No                      | OSPF goes DOWN after reload of VPN Peer                                  |
| CSCsj03706  | No                      | activex or java filter suppresses the syslog message 304001              |
| CSCeh98117  | No                      | Tunnel-group/ldap-login passwords in cleartext when viewed with more     |
| CSCsi98786  | No                      | Potential HW failure: Traceback in Thread Name: Dispatch Unit            |
| CSCsj14865  | No                      | SMTP fixup consistently drops '250 Ok' SMTP reply                        |
| CSCsh21462  | No                      | esmtphlo masking drops packet instead of masking                         |
| CSCek21850  | No                      | SIP: Stanby PIX show the wrong value of xlate timeout for sip media.     |
| CSCsd31162  | No                      | PPPoE: debug ppp doesn't display any debug messages                      |
| CSCse96428  | No                      | PIX/ASA drops packets with IP Option Router Alert set                    |
| CSCse99033  | No                      | tracked route removed from Standby firewall after failover               |
| CSCsh43799  | No                      | SIP Invite does not go to connect state in SIP Trunk Scenario            |
| CSCsh60480  | No                      | Unable to disconnect a call immediately with ip-address-privacy cmd      |
| CSCsh64554  | No                      | TCP sessions to the box denied because TCP connection limit exceeded     |
| CSCsh91283  | No                      | ASA/PIX: SunRPC inspect dropping packets on 7.0.6                        |
| CSCsi00628  | No                      | CPU utilization spike observed with ASDM connected                       |
| CSCsi27609  | No                      | ASA may drop MESSAGE requests due to sip-invite timeout                  |
| CSCsj12938  | No                      | PIX/ASA - show ip audit count - signatures 6050 - 6053 are Informational |
| CSCsj18055  | No                      | Traceroute fails through ASA if outside interface is pppoe and doing PAT |
| CSCsh55107  | No                      | DHCP relay fails when static translation for all hosts configured        |

## Related Documentation

Use this document in conjunction with the PIX firewall and Cisco VPN client Version 3.x documentation at the following website:

[http://www.cisco.com/en/US/products/sw/secursw/ps2120/tsd\\_products\\_support\\_series\\_home.html](http://www.cisco.com/en/US/products/sw/secursw/ps2120/tsd_products_support_series_home.html)

[http://www.cisco.com/en/US/products/sw/secursw/ps2308/tsd\\_products\\_support\\_series\\_home.html](http://www.cisco.com/en/US/products/sw/secursw/ps2308/tsd_products_support_series_home.html)

## Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

---

This document is to be used in conjunction with the documents listed in the “[Related Documentation](#)” section.

CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, *Packet*, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0705R)

© 2007 Cisco Systems, Inc.  
All rights reserved.